

lot Gateway " ເມເພີ

Contents

1. TECHNICAL SUPPORT	3
2. VISUAL SYMBOLS DEFINITION	3
3. ACRONYMS AND ABREVIATIONS	4
4. QUICK PRODUCT DESCRIPTION	5
4.1-UNBOX YOUR WILOW IOT 4G GATEWAY	5
4.2-ACCESSORIES DESCRIPTION	5
5. INSTALLATION	6
6.DEFAULT SETTINGS	10
7.HAVE ACCESS TO YOUR 4G ROUTER	12
7.1 -SIM CARD CONFIGURATION	12
7.2-MAKE SURE THAT THE DHCP SERVER IS ENABLED IN YOUR ROUTER	14
7.3-CONFIGURE THE WIFI ACCESS POINT	15
7.3.1-Router Settings With WDS	15
7.3.2-Router Settings Without WDS	16
7.4-ENABLE THE MQTT PROTOCOL	16
7.5-BEANDEVICE® WILOW® CONFIGURATION	16
7.6-BEANSCAPE [®] RA CONFIGURATION (REMOTE ACCESS)	21
8.WHERE TO FIND MORE TECHNICAL INFORMATION	23



DISCLAIMER

The information contained in this document is the proprietary information of BeanAir[®].

The contents are confidential and any disclosure to persons other than the officers, employees, agents or subcontractors of the owner or licensee of this document, without the prior written consent of BeanAir[®] GmbH, is strictly prohibited.

BeanAir[®] makes every effort to ensure the quality of the information it makes available. Notwithstanding the foregoing, BeanAir[®] does not make any warranty as to the information contained herein, and does not accept any liability for any injury, loss or damage of any kind incurred by use of or reliance upon the information.

BeanAir[®] disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

BeanAir[®] reserves the right to make modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to programs and/ or equipment at any time and without notice.

Such changes will, nevertheless be incorporated into new editions of this document. Copyright: Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights are reserved.

Copyright © BeanAir GmBh 2022

1. TECHNICAL SUPPORT

IOT Gateway [®] ^L

For general contact, technical support, to report documentation errors and to order manuals, contact BeanAir[®] Technical Support Center (BTSC) at: tech-support@beanair.com

For detailed information about where you can buy the BeanAir[®] equipment/software or for recommendations on accessories and components visit: www.beanair.com

To register for product news and announcements or for product questions contact BeanAir's Technical Support Center (BTSC).

Our aim is to make this user manual as helpful as possible. Please keep us informed of your comments and suggestions for improvements. BeanAir® appreciates feedback from

2. VISUAL SYMBOLS DEFINITION

Symbols	Definition
	Caution or Warning – Alerts the user with important information about BeanAir [®] wireless IOT Sensors. if this information is not followed, the equipment /software may fail or malfunction
	Danger – This information MUST be followed if not you may damage the equipment permanently or bodily injury may occur.
Ù	Tip or Information – Provides advice and suggestions that may be useful when installing BeanAir Wireless IOT Sensors.



3. ACRONYMS AND ABREVIATIONS

Advanced Encryption Standard				
Clear Channel Assessment				
Carrier Sense Multiple Access/Collision Avoidance				
Guaranteed Time-Slot				
Kilo samples per second				
Low duty cycle data acquisition				
Logical Link Control				
Link quality indicator				
Media Access Control				
Packet error rate				
Power Over Ethernet				
Radio Frequency				
Secure Digital				
Uninterruptible power supply				
USB On The Go				
Wireless DAQ				
Wireless Sensor Networks				

lot Gateway ° <u>wil</u>iw

4. QUICK PRODUCT DESCRIPTION

4.1 UNBOX YOUR WILOW IOT 4G GATEWAY

Wilow IOT Gateway is available in three versions:

- WILOW-IOT-GATEWAY-4G-MPWR, Mains Power supply
- WILOW-IOT-GATEWAY-4G-WDS-MPWPR, Mains power supply, WDS function
- WILOW-IOT-GATEWAY-4G-SOLAR, Solar Power Supply WILOW-IOT-GATEWAY-4G-SO-

LAR, with Solar Power Supply

The difference between the Mains power version and the solar panel version, is that the WDS function is only available on the Mains power version.

So users who works with the solar power supply version canot use the WIFI bridge because there is no WDS options which is available.

It is provided with a 4G/LTE antenna, WiFi antenna, external cables for both WiFi & 4G/LTE antennas and a power supply plug

4.2 ACCESSORIES DESCRIPTION

In addition to the WiLow® IoT gateway you will find inside the packet a list of accessories:

- 4G/LTE Antenna
- WiFi Antenna
- External cable for Wifi antenna
- External cable for 4G/LTE antenna
- Power supply plug

4.2 ACCESSORIES DESCRIPTION

Wilow[®] IOT Gateway



For more info on the accessories and its specification please refer to the user manual

5. INSTALLATION

1 : Please follow the following wiring code instructions to correctly build your own AC Power supply

• MAINS POWER SUPPLY (HARDWARE VERSION BEFORE 15/05/2019)

The previous hardware version comes with a Female Socket and a Male Plug



lot Gateway [®] Wilew

QUICKSTART

• MAINS POWER SUPPLY (HARDWARE VERSION AFTER 15/05/2019)

The previous hardware version comes with a Male Socket and a Female Plug



• SOLAR POWER SUPPLY (HARDWARE VERSION AFTER 15/06/2019)



DC Power:

The solar power controller can work between 13VDC to 20VDC, user can use an AC/DC power adapter in this voltage rating.



If the DC Voltage is less than 13VDC, the provided voltage will not be enough to power the Solar Power Manager



1. Use the provided antennas cables and power supply cable to connect to the appropriate connectors as shown below in the figure.



2. Open the box enclosure and use the Ethernet cable to connect your Laptop to the router in order to configure the IoT Gateway and get it ready for remote monitoring, as well to insert SIM card. Use a screwdriver to remove the black lid and properly insert the SIM card.

SIM CARD INSERTION





3. Don't forget to turn On the switch mode box by pushing the ON/OFF push buton at the top left corner, in order to charge the Lead-Acid Battery and get the gateway ready for configuration.



4. Use an ethernet cable to connect the router inside the IOT Gateway[®] to your laptop.





6. DEFAULT SETTINGS

THE IOT GATEWAY® COMES WITH A DEFAULT IP ADDRESS: 192.168.1.243

Assign a static IP address to your PC within the same subnetwork as your IOT Gateway[®]
 In the search bar tap change ethernet settings, then click on open



• Click on change Adapter settings

Ethernet

Network 7 Connected Related settings Change adapter options

Change advanced sharing options





• Right click on the Etherner device with is connected to your IOT Gateway, choose Propreties



• Double click on Internet Protocol Version4 (TCP/IPv4)

This connection uses the following items:



- Enter the flowing settings:
 - Enter any ip in the form of 192.168.1.XXX where XXX is a number from 2 to 254 (except 243 which is the router IP address).
 - Enter 255.255.255.0 for your subnet mask
 - The default gateway must come with the same IP address that your 4G Router has **192.168.1.243**
 - Finally enter primary DNS server IP, the same than your 4G Router IP 192.168.1.243
 - Click on OK validate your configuration



Internet Protocol Version 4 (TCP/IP	v4) Properties	×	
General			
You can get IP settings assigned au this capability. Otherwise, you need for the appropriate IP settings.	tomatically if your network supports d to ask your network administrator		
Obtain an IP address automat	ically		
Use the following IP address:			
IP address:	192 . 168 . 1 . 244 ┥	-	 Your PC IP address
Subnet mask:	255.255.255.0		
Default gateway:	192 . 168 . 1 . 243	+	 Your router IP address
Obtain DNS server address au	tomatically		
Use the following DNS server a	addresses:		
Preferred DNS server:	192 . 168 . 1 . 243		
Alternate DNS server:	• • •		
Validate settings upon exit	Advanced		
	OK Cancel		

• Once your PC and IOT Gaetway[®] are connected to the same network, you can easily have access to the router.

7. HAVE ACCESS TO YOUR 4G ROUTER

Use your browser on your PC and log in to the router using the following settings:

- IP address: 192.168.1.243 (tap it in google search bar)
- Username: admin | password: Beanair2020!

7.1 SIM CARD CONFIGURATION

• To configure your 4G/LTE Router go on Network then Click on Mobile





• Now configure your mobile settings as follow

General	Network Operators	Mobile Data	a Limit				
Mobile (Configuration						
Mobile Co	onfiguration					Choose QMI conn QMI.	ection type because
SIM 1						QMI option is hig	hly recommended.
	Cor	nnection type	QMI 🗸 🔶				
		Mode	NAT 🗸			Check Auto APN a	nd the connection w
		Auto APN	Passthrough	and Bridge modes are disa	bled when multiman is en	bled Access Point Nam identifier used by GSM carrier	e (APN): is a configu a mobile device whe
		C	Connection will	be established automatically	6		
		PIN number	0000			Enter the right PII	N number and PUK co
		PUK code		+		Used this field on	lv if the SIM card's PI
	Dia	aling number	*99#			used	y in the only curd of in
		MTU	1500			Choose 1500	
	S	Service mode	Automatic	× •		Choose Automati	as a service mode
	Deny o	data roaming [. ←			Uncheck Denv dat	ta roaming option
						80.1251943679478488478545555 • 279485	
	Mobile Data (On Demand					
	mobile bata e	Demand	Enab	ole 🖌			
		No	data timeout (se				
	Force TE po	twork		-7			
	FOICE LIE HE	WOIK					
			Enab	ole 🕑			
			Reregist	er 🔲			
			Interval (se	ac) 300			
							Save



You can get the APN ID from your telecom operator provider

If an invalid PIN number was entered (i.e. the entered PIN does not match the one that was used to protect the SIM card), your SIM card will get blocked. To avoid such mishaps, it is highly recommended to use an unprotected SIM. If it happens and you insert a protected SIM and the PIN number is incorrect, your card won't get blocked immediately, although after a couple of reboots OR configuration saves it will

lot Gateway ° 💴

7.2 MAKE SURE THAT THE DHCP SERVER IS ENABLED IN YOUR ROUTER

• LAN IP address should be 192.168.243 by default and if this is not the case for whatever reason ,you will need to set it back to 192.168.1.243 in the configuration panel you can find it in the overview page

Local Network	₿
IP / netmask	Configuration 243 / 255.255.255.0
Clients connected	3

TELTONI	KA Status Ne	twork - Services	- System -	Logout⊡
LAN				
Configuration				
General Setup	Advanced Settings			
	IP address	192.168.1.243		
	IP netmask	255 255 255.0 *		
	IP broadcast			
DHCP Server				
General Setup	Advanced Settings			
	DHCP	Enable •		
	Start	100		
	Limit	143		
	Lease time	12	Hours *	
	Start IP address:	192.168.1.100		
	End IP address:	192.168.1.242		

7.3 CONFIGURE THE WIFI ACCESS POINT

7.3.1 Router Settings With WDS

• Wilow[®] IOT Gateway integrates a high gain WIFI Access point. This access point is already preconfigured with the following settings, however the access point settings on the router are disabled, so the WIFI connectivity will be provided by the WIFI Bridge:

AP IP address	192.168.1.20
AP Webserver Login	Ubnt
AP Webserver PW	Beanair2020!
WIFI SSID	Beanair
WIFI Password	Beanair2019
Encryption	WPA2-PSK, Cipher, Auto
WIFI RF Channel	Auto
AirMax function	disabled

• If you fail to access to the WIFI Bridge, just reset it to the factory settings.

To reset it to factory defaults, press and hold the Reset button for more than 10 seconds while the device is powered on.



- After the reset process the default login information is proved below:
 - Default IP Address (LAN IP): 192.168.1.20
 - Default User Name: ubnt
 - Default Password: ubnt

7.3.2 Router Settings Without WDS

• By default the WIFI access point is enabled with the following settings:

WIFI SSID	Beanair
WIFI Password	Beanair2019
AP Webserver PW	Beanair2020!
Encryption	WPA2-PSK, Cipher, Auto
WIFI RF Channel	Auto

7.4 ENABLE THE MQTT PROTOCOL

• Under services tab ,go to MQTT Broker and make sure it is enabled and using Local port 1883 (make sure this port is not used by other application)

TELTONIKA Status Net	work - Services -	System -	Logout 🖻
Broker Publisher			
MQTT Broker			
Enable			
Local Port	1883		
Enable Remote Access	×		
Broker settings			
Security Bridge Miscellaneous			
Use TLS/SSL			

7.5 BEANDEVICE® WILOW® CONFIGURATION

• Connect your Wilow[®] BeanDevice[®] to your laptop using the USB cable, turn it on using the magnet, run the BeanScape[®] supervision software Wilow[®] then go to (Tools --> WIFI network settings), enter the default network settings and click on validate.





- Default SSID: Beanair
- Password: Beanair2019
- security type: WPA2-PSK

Beanair 🗸
Beanair2019
WPA2 ~
REGION_EU ~

• Add BeanScape to firewall, from tools click on Advanced Settings then Add to Firewall

BeanScape File Server	Тоо	ls Off. Data Analysis Advance		
📓 📓 🙆		BeanScape® Configuration		
MAC_ID :		Alarm window		
📒 Ch_X		Wifi Network Settings	Advanced Settings	
Ch_Y		Export/import settings		
GI_Z		SNTP Client Configuration		
		Alarm Management	Firewall	Validate
		Notification Management	T II CWAII	Validate
	۲	Offline graph	1	
	0	Date conversion	Matlab Functions	Check Download
		Advanced Settings		
		MQTT Configuration		
I	_		Sql Server Report	Check Install

• Now start the BeanScape[®] Server by clicking directly on the Green button or selecting Start the server from the Server option on the Menu bar

👾 Bear	nScape				🖛 Bea	nScape			
File	Server	Tools	Off. Data	Analys	File	Server	Tools	Off. Data Analysis	Help
: 🔒 📊	Sta	rt the ser	ver			a 🗾	2 🔘	0	
	Ser	ver wind	ow			Sta	art the se	rver	





.

• The BeanDevice profile will be displayed on your screen



• Next, start MQTT configuration panel on BeanDevice® tab

File Server Tools Data Analysis	BeanDevice Help
Image: Second secon	Enable measure log Disable measure log Reset measure memory cache for all the sensors Display Wireless Network Information Sensor Conf
INC_Y	MOTT

Figure 29 :BeanDevice MQTT module configuration



• MQTT configuration window will pop up:

lot Gateway ° 💴

Broker 1883 MQTT Satus: Stopped Stopped Stopped MQTT Satus: Stopped MQTT Satus: Stopped MQTT Satus: Stopped MQTT Satus: MQTT Satus: Stopped MQTT Satus: MQTT Satus: Stopped MQTT Satus: MQTT Satus: MQTT Satus: Stopped MQTT Satus: Stopped MQTT Satus: MQTT Satus: Stopped Cater Validate Cater Validate Cater Validate Cater Validate Validate Cater Validate Validate Cater Validate Validat	MQTT Module : MAC_ID : 0 x A4D57843DED30000				X
IP Broker: 192.153.1243 Import Restart DNS: Import Validate Topic for static measurement Publish Status: Import Import Publish Status: Import Import Publish Status: Import Import </td <td>Broker Port: 1883 DNS Status: Disabled </td> <td>MQTT Status MQTT</td> <td>s Status: Stopped</td> <td>Stop ~</td> <td>Validate</td>	Broker Port: 1883 DNS Status: Disabled	MQTT Status MQTT	s Status: Stopped	Stop ~	Validate
DNS Import Authentication Usemanne: Password: Validate SSL/TLS Corfig Security Protocol Vension: SSL/ALS Corfig Copher: Validate Validate Validate Topic for dynamic measurement MQTT Status: File Status Validate config Certif Certif Certif Certif Cafile Name: NA Upload Status NA Upload Status NA Upload Status NA Cancel and reset Byte Transferred Ora Ora Validate Validate	IP Broker: 192.168.1.243	MQ	TTACK: NA		Restart
Authentication Usemanne: Password: Validate StL/TLS Config Security Protocol Version: SLV2LOP Validate config Certif Certif Certif Certif Certif Certif Certif Certif Certif Certif Certif File Status NA Upload Status NA Decel and reset Byte Transferred Dytate Decel an	DNS:	Topic for stat	tic measurement		
Authertication Usemane: Password: Validate SSL/TLS Config Security Protocol Version: SSLV3_U Cpher: Validate config Cettif Cettif Cettif Cettif Cafle Name: NA CAfle Name: NA Cafle Valid from: NA Upload Status NA Cancel and reset Byte Transferred Progress 0% Subscription status: File Status NA Cancel and reset Byte Transferred Byte Transferred Doress D72 Validate	r Import Validate	Publi	sh Status: Enabled		
Usemame: AdD57843DED30000/SERSOR70 Default Password: Validate SSUTLS Config Security Protocol Version: SSLv3.0 Cipher: Validate config Certif Certif Caffe Name: NA CAffe Name: NA Caffe Name: NA Caffe Status Upload Status File Status NA Cancel and reset Didate Validate Ora Validate Validate Validate	Authentication	ID	Channel:	un_z ∨	
Password: Validate SSLTLS Config SSLTLS Config Security Protocol Version: SSLV3_0	Usemame:	Τορ	pic Name: A4D57843DED30000/SEN	SOR/0	Default
Valdate Topic for dynamic measurement SECurity Protocol Version: Situ3_0 Centri Validate config Certri Validate Certri Validate Certri Validate Certri Validate Certri Validate Certri Validate To NA Validate Validate Validate Va	Password:				Validate
SSL/TLS Config Security choice: Disabled Security choice: Disabled Security choice: Disabled Centri Validate config Certificate: CAfie Name: NA CA fie Valid from: NA To: NA Fie Status Upload Status NA Cancel and reset Disabled OT, MQTT Status: Image: Control MQTT Status: Image: Control Validate config Certificate: Cancel and reset Upload Status NA Cancel and reset Distatus Validate OT Validate OT Statt Validate Validate Validate Image: Control Statt Validate Validate <t< td=""><td>Validate</td><td>Topic for dyn</td><td>amic measurement</td><td></td><td></td></t<>	Validate	Topic for dyn	amic measurement		
Security choice: Usebled Disabled Control Version: Students Control Version: Students Control Version: Students Control Version: Validate config Cetti Cetti Cetti Cetticate: CAfie Vale CA	SSL/TLS Config	MOTT	Status: Enabled		
Security Protocol Version: Stav3 0 SSLv3 0 Validate Cpher: Validate config Cetti Cetti Cetticate : Validate config CA file Name: VA CA file Name: VA CA file Valid from: NA To : NA File Stavs NA Upload Status NA Cancel and reset Byte Transferred Progress 0 0%	Security choice : Disabled Disabled	•		AMUNIC	Default
Copher: Validate config Certif Certif <td>Security Protocol Version: SSLv3_0 SSLv3_0</td> <td>- Streaming</td> <td>g Topic: A40373450E0300075The</td> <td>AMING</td> <td>Validata</td>	Security Protocol Version: SSLv3_0 SSLv3_0	- Streaming	g Topic: A40373450E0300075The	AMING	Validata
Validate config Subscription Certif Subscription status: Enabled CAfie Name: NA Default CAfie Name: NA Validate CAfie Valid from: NA Validate CAfie Valid from: NA Validate Upload Status Start Start File Status NA Cancel and reset Byte Transferred 0% Validate	Cipher : Automatic		<u>k</u>		validate
Validate config States of the Name : M4D57843DE030000/07AC Default CAfile Name : NA Validate Validate CAfile Name : NA Validate Validate CAfile Valid from : NA Validate Validate Upload Status Start Start Validate File Status NA Cancel and reset ID Client: Validate Byte Transferred 0% Validate Validate		- Subscription			
Certif Image: Certificate : Ima	Validate config	Subscription	Tstatus.		
CA file Name : NA CA file Name : NA CA file Name : NA To : NA Upload Status Upload Status NA Defe Transferred Byte Transferred Progress 07, Validate Validate Validate Validate Validate Validate Validate Validate Validate Validate Validate Validate Validate Validate	Certif	Topic	c Name: A4D57843DED30000/OTA		Default
CA the Name: NA CA file Valid from: NA To: NA Upload Status Start File Status NA Upload Status Cancel and reset Byte Transferred D7,		♣- <u><</u>			Validate
CA file Valid from: Local Keep Alive Keep Alive Interval : 50 60 Upload Status NA Start Version: V3R1R1 V3R1R1 V Upload Status NA Cancel and reset Interval : 60 Interval : 50 60 Upload Status NA Cancel and reset Variant Validate Interval : 10 Units Interval : 10 Interval : 10 Validate	CAtle Name : Ma				
Upload Status Upload Status IFIe Status Upload Status NA Cancel and reset Diversion: Umain Cancel and reset Upload Status Upload		Keep Alive	Interval - 60	60	
Start Version: V3R1R1 File Status NA Upload Status NA Byte Transferred Cancel and reset Progress 0%	Upload Status			00	
The Status Cancel and reset Auto gen.ID Client: Image: Cancel and reset Upload Status NA Cancel and reset ID Client: Image: Cancel and reset Byte Transferred Image: Cancel and reset ID Client: Image: Cancel and reset Progress 0% Validate	Ele Cheture NA	Start	Version: V3RIRI	V3R1R1 ~	
Byte Transferred ID Client: WIL05588401638365481163 Process 0%	Unload Status NA Cancel	and reset Auto.gen.I	D Client: 1		
Process 0% Validate	Byte Transferred		D Client: WILO558840163636548116	3	
	Progress 0%			Validate	

• Follow these following screenshots and fill in your settings, then validate.

Broker Port:	1883	1883
DNSStatus:	0	
Brokerlp:	192.168.1.243	192.168.1.243
DNS:		
	Import	Validate



• Here you can check your MQTT different status, connected, stopped , connecting or disconnecting and can start your connection from here.

MQTTSTATUS			
MQTT Status:	Connecting	Start 👻	Validate
MQTT Ack:	NA		Restart

• LCDC topic is a string used by the broker to filter messages for each LowDutyCycle channel of the connected BeanDevice, enable each channel and set its name to default to avoid problems. Then validate

Topic Ldc Ldca		
Publish_status:	enabled	
Channel ID:	0 Ch_Z ~	
Topic Name:	F4B85E00A4D00000/SENSOR/0	Default
		Validate

• Streaming topic is a string used by the broker to filter messages for streaming data from the connected BeanDevice. Enable and set its name to default then validate

Streaming topic		
Publish_status:	enabled	
Streaming Topic	F4B85E00A4D00000/STREAMING	Default
		Validate

This Topic will be the string we will use to connect to the BeanDevice from remote BeanScape supervision software in order to send OTACs. By default this will be set to MAC_ID/OTAC.

• Enable subscribe and set your Topic to default and validate.

IOT Gateway[®]

Subscription Subscription status:	Enabled		
Topic Name:	A4D57843DED30000/OTAC		Default
			Validate

7.6 BEANSCAPE® RA CONFIGURATION (REMOTE ACCESS)

Using BeanScape[®] RA you will have the ability to subscribe remotely to any BeanDevice[®] publishing data, first you have to install and run your BeanScape RA at your monitoring office

• You have to switch to MQTT using this button

👐 Bea	nScape			
File	Server	Tools	Data Analysis	Help
:	🛃 🗹	2 💿		
		S	witch To MQTT	I

• Next ,go to Tools tab -->MQTT configuration and a new configuration window will pop up ,and you will establish a communication with your IoT Gateway ,

😵 MQTT Configuration				×_×		\times
MQTT Configuration Use DNS DNS: Broker IP 1977.8139 137 Port: 1893	197.8.139.137 1883	MQTT Connection MQTT Status MQTT Ack Enable MC	In A Contract of the second se	Start		
User Name Plane Password		Add Device Device Mac ID MAC ID	Select Device		•	
Validate Delete BeanDevice BeanDevice Select device	 ✓ Clear all ✓ 	Торіс	主 Valida	ite		



- Port should be set to 1883
- In Broker IP you have to enter the IoT Gateway Public IP Address, then validate
- From MQTT connection, enable MQTT by clicking on start button

MQTT Status Connected MQTT Ack ClientAccepted Disable MQTT	MQTT Connection		
MQTT Ack ClientAccepted	MQTT Status	Connected	
Dieshle MOTT	MQTT Ack	ClientAccepted	
Jodulo mari	Disable MQ	TT 🚺 Stop	

• Now, enter the BeanDevice[®] Wilow[®] MAC_ID and Subscribe to the same Topic that we had previously setup for the BeanDevice, then validate

Add Device Device Mac ID	F4B85E00A4D00000	- 🔟
MAC ID	F4B85E00A4D00000	
Topic	F4B85E00A4D00000/OTAC	
	🛨 Validate	
Request sent Suc	cessfully	

• Close the MQTT configuration window and make sure the server is started, the BeanDevice will be at your disposal, to read measurement,





8. WHERE TO FIND MORE TECHNICAL INFORMATION?

For more technical litterature, please visit our White Paper Page:

Please refer to the BeanDevice[®] 2.4GHz EcoSensors user manual section for more information https://www.wireless-iot.beanair.com/files/UM-RF-03-ENG-EcoSensor-Wireless-Sensors-for-En-

For detailed information on the available Data Acquisition mode ,please refer to our technical note http://www.wireless-iot.beanair.com/files/TN-RF-008-Data-acquisition-modes-available-onthe-BeanDevice.pdf

Facing technical problems ? Contact our technical support team at : tech-support@beanair.com



